Procedure No. 2205.11: Audit Vulnerability Scan
Reference: Policy No 2205
Effective Date: 12/28/04
Prior Issue: N/A

Purpose

The Arizona Department of Juvenile Corrections (ADJC) Management Information Systems (MIS) may conduct audits to:

- Ensure integrity, confidentiality and availability of information and resources;
- Investigate possible security incidents ensure conformance to ADJC security policies;
- Monitor user or system activity where appropriate.

This Procedure covers all computer and communication devices owned or operated by ADJC and any computer and communications device that are present on ADJC premises which may not be owned or operated by ADJC.

Rules:

1. **MIS** shall utilize approved software to perform electronic scans of Client's networks and/or firewalls or on any system at ADJC.

2. **MIS** shall provide protocols, addressing information, and network connections sufficient for and audit to utilize equipment to perform network scanning. This access may include:
   a. User level and/or system level access to any computing or communications device;
   b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on ADJC equipment or premises;
   c. Access to work areas (labs, offices, cubicles, storage areas, etc.);
   d. Access to interactively monitor and log traffic on ADJC networks.

3. **MIS** shall conduct routine network audits on network security, user ids, performance, access, and other network information as deemed important

4. The **MIS** shall submit an annual IT (Information Technology) Security Assessment to Government Information Technology Agency (GITA**)** (P800-S805) addressing twenty-one categories of risks:
   a. Standards;
   b. Risk Management;
   c. Account Management;
   d. Configuration Management
   e. Authentication;
   f. Session Controls;
   g. Network Security;
   h. Modems;
   i. Encryption Technology;
   j. System Administration;
   k. Incident Response Capability;
   l. Auditing;
   m. Virus Protection;
   n. Business Continuity and Disaster Planning
   o. Backups;
   p. Maintenance;
   q. Labeling;
   r. Media Sanitizing/Disposal;
   s. Physical Security;
   t. Personnel Security;
   u. Training & Awareness.

5. **MIS NETWORK SECURITY TEAM** shall scan the network to address unsecured network access points of entry, server and workstation vulnerabilities, LAN/WAN network vulnerabilities, Wireless vulnerabilities, and other points of network security related interest as technology changes at least on a yearly basis or if it is determined one is needed. If the MIS Security team does not have the resources to scan their network, **MIS** shall contract the work out. The contracting company will sign an agreement and acknowledge that ADJC authorizes this contracted company on State Contract to use ADJC's networks as a gateway to conduct these audit tests during the dates and times outlined in the contract. Any positive findings from the scanning event report shall be repaired and submitted to GITA for evaluation with noted corrections on repairs or submit a plan to repair the findings if it cannot be completed in time for submittal.

6. **MIS** shall make available network services for external State Agencies deemed responsible by GITA for performing scanning audits when requested.

7. Network performance and/or availability may be affected by the network scanning. **ADJC** shallrelease any externally contracted company of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result in gross negligence or intentional misconduct.

8. **ADJC** shall identify in writing a person to be available if the result of the Scanning Team has questions regarding data discovered or requires assistance.

9. **ADJC AND SCANNING TEAM** shall identify in writing the allowable dates for the scan to take place.

10. **ANY EMPLOYEE** found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Effective Date:	Approved by Process Owner:	Review Date:	Reviewed By: